Publ. Mat. (2007), 165–180
Proceedings of the *Primeras Jornadas de Teoría de Números*.

VOLCANOES OF ℓ-ISOGENIES OF ELLIPTIC CURVES OVER FINITE FIELDS: THE CASE $\ell = 3$

J. M. Miret, D. Sadornil, J. Tena, R. Tomàs, and M. Valls

Abstract

This paper is devoted to the study of the volcanoes of ℓ-isogenies of elliptic curves over a finite field, focusing on their height as well as on the location of curves across its different levels. The core of the paper lies on the relationship between the ℓ-Sylow subgroup of an elliptic curve and the level of the volcano where it is placed. The particular case $\ell = 3$ is studied in detail, giving an algorithm to determine the volcano of 3-isogenies of a given elliptic curve. Experimental results are also provided.

1. Introduction

Isogenies are an important tool in the study of the geometry and arithmetic of elliptic curves over finite fields. On the one hand, the search of kernels of isogenies of a given elliptic curve E plays a central role in the improvements introduced by Elkies and Atkin to the Schoof algorithm (referred to as the SEA algorithm [**1**], [**3**], [**9**], [**14**]), which computes the cardinal of the group of rational points of E. On the other hand, since such a cardinal is an isogeny invariant, computing the isogenies of a given elliptic curve E provides us with curves which have the same cardinal. This can be useful for cryptographic purposes.

Anyway, notice that only isogenies with prime degree ℓ need to be considered. This is due to the fact that any isogeny of degree $d = d_1 d_2$ can be constructed as a composition of isogenies of degrees d_1 and d_2. In fact, an upper bound for the size of the prime ℓ is known [**5**].

Kohel [**7**] pointed out that the relationship between ℓ-isogenous elliptic curves, for ℓ prime, can be represented by means of a graph so called *volcano* (due to its special features). He takes advantage of this structure to determine the endomorphism ring (i.e. its conductor) of a given elliptic curve, whose cardinal m is known.

2000 *Mathematics Subject Classification.* 14H52, 14K02, 11G20, 11T71.
Key words. Elliptic curves, finite fields, isogenies, volcanoes, ℓ-Sylow subgroup, algorithms.
Supported by the grants TIC2003-09188 and MTM 2004-008076 (Spain).

Later on, volcanoes of isogenies are also considered by Fouquet and Morain [**4**] to obtain computational simplifications for the SEA algorithm. In particular, they determine the height of the volcano using exhaustive search over several paths on the volcano to detect the crater and the floor levels. For this purpose, they compute the roots of ℓ-modular polynomials.

The aim of this paper is further exploiting these ideas in order to study the ℓ-isogenies of elliptic curves. In particular, we approach the problem of obtaining the structure of the volcano of ℓ-isogenies (and hence its height), taking advantage of the knowledge of the ℓ-Sylow subgroup of the elliptic curves. So, while Kohel [**7**] shows the relationship between levels of the volcano and the endomorphism ring of the curves at those levels, we relate such levels with the ℓ-Sylow subgroup structure of the curves.

It should be pointed out that the height can be straightforwardly obtained in most of the cases (those called *regular* volcanoes). Moreover, for the non-regular ones, this procedure avoids the costly descent until the floor level, required in the Fouquet-Morain's algorithm.

Furthermore, we also study in more detail the particularities of the case $\ell = 3$, extending a previous work for the case $\ell = 2$ [**12**]. Results of an efficient implementation of the algorithm for the computation of the volcano of 3-isogenies are provided. For this particular case, the algorithm can take benefit of the usage of the Vélu formulae for the computation of the isogenous curves.

2. Volcanoes of ℓ-isogenies

Let E be an elliptic curve over a finite field $\mathbb{F}_q$. Then, given a rational subgroup $G \subseteq E(\mathbb{F}_q)$ there exists a unique (up to isomorphism) elliptic curve E' and a rational morphism $\mathcal{I}\colon E \to E'$ with kernel G. Such a morphism is referred to as an *isogeny* between E and E' [**15**]. Then, we talk about an ℓ-isogeny when the cardinal of G is ℓ (which is the degree of the isogeny).

In fact, the endomorphism ring $\mathcal{O}$ of an ordinary elliptic curve E can be identified as an order in an imaginary quadratic field K [**6**], [**15**]. Hence, if $\mathcal{I}\colon E \to E'$ is a rational isogeny of prime order ℓ ($\ell \neq p$), Kohel [**7**] shows that $[\mathcal{O}:\mathcal{O}'] = 1, \ell, \frac{1}{\ell}$. Depending on each case, Kohel denotes the isogeny $\mathcal{I}$ as *horizontal, descending* or *ascending*, respectively.

As it is known [**7**], this notion of direction induces, in the set of isomorphism classes, a stratified graph structure, where arcs represent the horizontal, descending or ascending ℓ-isogenies between classes of elliptic curves.

In particular, it can be noticed that each connected component of the graph of ℓ-isogenies can be shaped like a *volcano*. The top level of the volcano is a cycle, denoted *crater*, such that from each of its vertices hangs an $(\ell-1)$-complete tree, all of them isomorphic one to each other. The vertices at the bottom level have only one outgoing arc, which is ascending (unless when the volcano has exactly one level, in which case each node has one or two horizontal outgoing arcs). In the other cases each vertex has $\ell+1$ outgoing arcs: for the vertices in the *volcanoside*, one is ascending and ℓ are descending, while for the vertices on the crater it will depend on whether its length is 1, 2 or greater. Moreover at each level all the curves have the same endomorphism ring. Figure 1 shows the general structure of such a volcano for the case $\ell = 3$.

Then, the remaining of this section is devoted to the study of the properties of these volcanoes of ℓ-isogenies of elliptic curves, $\ell > 2$, having an ℓ-order subgroup generated by a rational point P, focusing on their height and on the location of the curves over the different levels. Forthcoming work will extend this study to the case of a rational group generated by a non-rational point. Nevertheless, as we will see, the case $\ell = 3$ can be completely studied, by taking twisted curves when the curve has rational 3-order subgroups with non-rational points.

2.1. Height of the volcanoes.

Let E be an ordinary elliptic curve over $\mathbb{F}_q$ with group order m and $\mathcal{O}$ the endomorphism ring of E. Then $\mathcal{O}$ is an order of the imaginary quadratic field $K = \mathbb{Q}(\sqrt{t^2-4q})$ [**6**], where t is the trace of Frobenius endomorphism π of E. Notice that if d is the squarefree part of the discriminant $d_\pi = t^2 - 4q$ of the Frobenius endomorphism π, that is to say $d_\pi = f_0^2 d$, then it follows [**7**] that the conductor f of the order $\mathbb{Z}[\pi]$ corresponds to $f = f_0$ if $d \equiv 1 \pmod 4$ and $f = f_0/2$ otherwise. The ring of integers of K is $\mathcal{O}_K = \mathbb{Z} \oplus \mathbb{Z}\omega$ where

$$\omega = \begin{cases} \dfrac{1+\sqrt{d}}{2}, & d \equiv 1 \pmod 4, \\ \sqrt{d}, & d \equiv 2,3 \pmod 4. \end{cases}$$

Since $\pi \in \mathcal{O}_K$, there exists an integer a such that the Frobenius endomorphism π satisfies

$$\pi = a + f\omega.$$

If we consider the volcano V_E associated to the curve E, since all the elliptic curves in this volcano have the same order m, all of them determine the same integers a, f and the same element ω. So, the height $h(V_E)$

of the volcano of ℓ-isogenies will just depend on these elements. More precisely, one can deduce from [**4**], [**17**] that

$$h(V_E) = v_\ell(f).$$

Hence, in order to analyze the height of a volcano it will be useful to study the features of f. Therefore, the study of the ℓ-adic valuation of d_π will provide some knowledge on $v_\ell(f)$.

In the following we will always suppose that the elliptic curves have a rational point of order $\ell > 2$ (so $v_\ell(m) \geq 1$). The case $\ell = 2$ is already studied in [**12**].

Theorem 1. *Let E be an elliptic curve over $\mathbb{F}_q$ of order m and $\ell > 2$ a prime number such that $v_\ell(m) \geq 1$.*

If $v_\ell(q-1) \geq 1$ then:

i) *If $v_\ell(m) > 2v_\ell(q-1)$, then $h(V_E) = v_\ell(q-1)$.*
ii) *If $v_\ell(m) = 2v_\ell(q-1)$, then $h(V_E) \geq v_\ell(q-1)$.*
iii) *If $v_\ell(m) < 2v_\ell(q-1)$, then either $h(V_E) = (v_\ell(m)-1)/2$ when $v_\ell(m)$ is odd or $h(V_E) = v_\ell(m)/2$ when $v_\ell(m)$ is even.*

Otherwise, if $v_\ell(q-1) = 0$ then $h(V_E) = 0$.

Proof: Taking into account that $t^2 - 4q = (q-1)^2 - m[m-2(q-1)-4]$, it follows that $v_\ell(t^2-4q) \geq \min\{2v_\ell(q-1), v_\ell(m)\}$. The value $v_\ell(t^2-4q)$ is determined, unless in the case that $2v_\ell(q-1) = v_\ell(m)$. This situation causes that, for the second case, only a lower bound of the value of the height can be given. Concerning the third case, there exist two possible values of the height, depending on the parity of $v_\ell(m)$.

In the case $v_\ell(q-1) = 0$, we obtain $v_\ell(t^2-4q) = 0$. But moreover, it turns out that $t^2 - 4q$ is a square residue modulus ℓ. Then the modular polynomial $\phi_\ell(x, j)$, being j the j-invariant of E, has exactly two roots [**2**], that is, E has two ℓ-isogenies. Therefore, E must be at the crater of the volcano and, since that is the situation for all curves of the volcano, it follows that $h(V_E) = 0$. □

2.2. Location of the curves on V_E according to their ℓ-Sylow subgroup.

Now we are going to give some more details about the structure of the volcanoes of ℓ-isogenies according to the ℓ-Sylow subgroups of the curves involved. Firstly, notice that the curves on the floor are precisely those whose ℓ-Sylow subgroup is cyclic, because they are the only ones that have one or two ℓ-isogenies (this last case appears when the crater coincides with the floor).

Let E be an ordinary elliptic curve over $\mathbb{F}_q$ with group order m, $\mathcal{O}$ its endomorphism ring and π its Frobenius endomorphism. As mentioned in Subsection 2.1, the Frobenius endomorphism can be written as $\pi = a + f\omega$, where a satisfies [**7**]

$$a = \begin{cases} \dfrac{t-f}{2}, & d \equiv 1 \pmod 4, \\ \dfrac{t}{2}, & d \equiv 2,3 \pmod 4. \end{cases}$$

From Lenstra [**8**] and Wittmann [**17**] it follows that $E(\mathbb{F}_q) \cong \mathcal{O}/(\pi - 1)$ as $\mathcal{O}$-modules, from where one can deduce that $E(\mathbb{F}_q) \cong \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z}$, where $n_2 = \gcd(a-1, f/g)$, $n_2 \mid n_1$, $n_2 \mid (q-1)$, $m = n_1 n_2$ and g is the conductor of $\mathcal{O}$. Then, we can also deduce the following result.

Proposition 2. *Let E be an elliptic curve over $\mathbb{F}_q$ with order m, $\mathcal{O}_K = \mathbb{Z} \oplus \mathbb{Z}[\omega]$ and $\pi = a + f\omega$, for some $a \in \mathbb{Z}$. Then, $v_\ell(a-1) \geq \min\{v_\ell(f), v_\ell(m)/2\}$.*

Proof: If $d \equiv 2,3 \pmod 4$, since $a = t/2$, we get $(a-1)^2 = f^2 d + m$. Otherwise, $a = \frac{t-f}{2}$ and, since $(t-2)^2 = f^2 d + 4m$, we get $4(a-1)^2 = 4m + f^2(d-1) - 4f(a-1)$. Considering the ℓ-adic valuations of these expressions, the claim follows. □

Then we can gain some insight about the location of the given curve E in the volcano according to their ℓ-Sylow subgroup

$$S_\ell(E(\mathbb{F}_q)) = \{P \in E(\mathbb{F}_q) : \exists\, k \geq 0 \text{ s.t. } \ell^k \cdot P = 0_E\}.$$

Since it is a subgroup of $E(\mathbb{F}_q)$, its structure is $\mathbb{Z}/\ell^r\mathbb{Z} \times \mathbb{Z}/\ell^s\mathbb{Z}$, with $s \leq \min\{r, v_\ell(q-1)\}$.

Notice that from the former result it follows that the curves in the vertices of the same level have identical ℓ-Sylow group. Moreover, when ascending over the vertices of the volcano, the value of s either increases or remains unchanged. Then, taking into account Proposition 2 and the fact that $s \leq v_\ell(q-1)$, it is easy to prove the next result:

Theorem 3. *Let E be an elliptic curve over $\mathbb{F}_q$ of order m with $\nu = v_\ell(m) \geq 1$. Then the volcano V_E satisfies:*

i) *The ℓ-Sylow subgroup of the curves on the floor is $\mathbb{Z}/\ell^\nu\mathbb{Z}$.*

ii) *If ν is odd, the ℓ-Sylow subgroup of the curves on the i-th level is $\mathbb{Z}/\ell^{\nu-i}\mathbb{Z} \times \mathbb{Z}/\ell^i\mathbb{Z}$.*

iii) *If ν is even, the ℓ-Sylow subgroup of the curves on the i-th level is $\mathbb{Z}/\ell^{\nu-i}\mathbb{Z} \times \mathbb{Z}/\ell^i\mathbb{Z}$ for $1 \leq i \leq \nu/2$. Moreover, for the rest of levels (if any) until reaching the crater, the structure is $\mathbb{Z}/\ell^{\nu/2}\mathbb{Z} \times \mathbb{Z}/\ell^{\nu/2}\mathbb{Z}$.*

Notice that in the case that ν is even and the height of the volcano is greater than $\nu/2$, from level $\nu/2$ until the crater of the volcano the structure of the ℓ-Sylow group is unaltered, and it is equal to $\mathbb{Z}/\ell^{\nu/2}\mathbb{Z} \times \mathbb{Z}/\ell^{\nu/2}\mathbb{Z}$. This situation can not occur in the case ν odd, since the height is lower than $\nu/2$.

The level for which the structure of the ℓ-Sylow subgroup stabilizes is called *stability level* (which is $\nu/2$). Then, those volcanoes whose height is lower or equal than the stability level are referred to as *regular volcanoes* (see Figure 1).

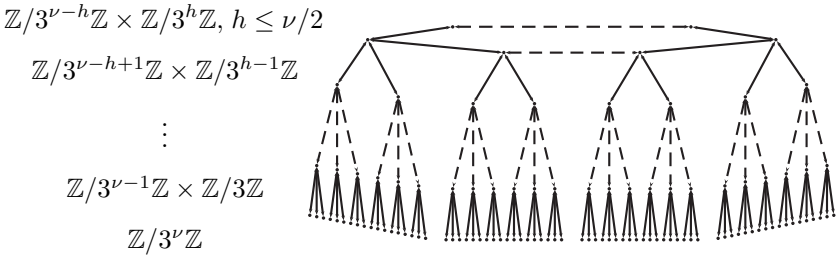

Figure 1. Structure of a regular volcano of 3-isogenies

3. The case $\ell = 3$

Notice that given an elliptic curve E over a finite field $\mathbb{F}_q$ with a rational subgroup of order 3 generated by a non-rational point P, then the twisted curve E' over $\mathbb{F}_q$ has a subgroup of order 3 whose points are rational. This is due to the fact that, since such a point P has a rational abscissa, either its ordinate or the ordinate of its corresponding point in E' are rational. Hence, as a consequence of this property, the case $\ell = 3$ turns out to be interesting enough, since a complete study of the volcanoes of 3-isogenies can be easily provided.

This section describes the basic techniques in order to design an algorithm to compute the volcanoes of 3-isogenies. Firstly, a suitable parametrization of curves with a rational point of order 3 is given. Secondly, in order to simplify computations, a representative curve of each isomorphism class is chosen. Then, the expressions of the isogenies are explicitly found using the Vélu formulae [**16**]. Finally, we can take benefit of the usage of a polynomial algorithm [**13**] which determines the structure of the 3-Sylow subgroup. This algorithm, as well as the one for determining the 2-Sylow subgroup of an elliptic curve (see [**11**]),

outputs the integers n and r such that the 3-Sylow subgroup of E is isomorphic to $\mathbb{Z}/3^n\mathbb{Z} \times \mathbb{Z}/3^r\mathbb{Z}$, $r \leq n$, and points P and Q of order 3^n and 3^r.

3.1. Curves with points of order 3.

The elliptic curves we are interested in are those with a rational point of order 3. Such elliptic curves have either 2 or 8 points of order 3. Taking one of these points as the origin, the equation of the curve can be expressed as follows:

$$E_{a,b} : y^2 + axy + by = x^3, \quad a, b \in \mathbb{F}_q.$$

Under this model, $(0,0)$ and $(0,-b)$ are points of order 3. Moreover, taking into account its 3-division polynomial $\Psi_3(x) = x(x^3 + a^2/3x^2 + 3abx + b^2)$, the structure of the subgroup of 3-torsion points can be easily obtained:

- If $v_3(q-1) = 0$, the factorization type of $\Psi_3(x)$ is $[1,1,2]$, but only the abscissa $x = 0$ gives two rational points of $E_{a,b}/\mathbb{F}_q$ and so $E_{a,b}(\mathbb{F}_q)[3] \cong \mathbb{Z}/3\mathbb{Z}$.
- If $v_3(q-1) > 0$, the factorization type of $\Psi_3(x)$ is either $[1,3]$ or $[1,1,1,1]$. In the first case $E_{a,b}(\mathbb{F}_q)[3] \cong \mathbb{Z}/3\mathbb{Z}$, while in the second $E_{a,b}(\mathbb{F}_q)[3] \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.

Concerning the isomorphism classes of the curves $E_{a,b}/\mathbb{F}_q$, a representative curve in each class can be obtained as follows:

- If $v_3(q-1) = 0$, each isomorphism class can be univocally represented by the curve $E_{1,\lambda}/\mathbb{F}_q$ (being $\lambda = \frac{b}{a^3}$), unless when $a = 0$, in which case the representative curve is $E_{0,1}/\mathbb{F}_q$.
- If $v_3(q-1) > 0$, two cases should be distinguished, according to the factorization type of $\Psi_3(x)$, either $[1,3]$ or $[1,1,1,1]$.
  - The first situation is similar to the previous one when $a \neq 0$, so the representative is $E_{1,\lambda}/\mathbb{F}_q$. Otherwise, curves with $a = 0$ belong to two different isomorphism classes: $E_{0,\delta_1}/\mathbb{F}_q$ and $E_{0,\delta_2}/\mathbb{F}_q$, being $\delta_1^{3^{v-1}}$ and $\delta_2^{3^{v-1}}$ the primitive cubic roots of 1, where $v = v_3(q-1)$.
  - In the second situation, when $a \neq 0$, there exist four different representatives of the type $E_{1,\lambda}$ in each class (due to the fact that now the origin can be translated to the other points of order 3). The algorithm takes the representative with smallest value λ. In the case $a = 0$, the representative of the isomorphism class is $E_{0,1}/\mathbb{F}_q$. Equivalently, also $E_{1,\frac{1}{24}}/\mathbb{F}_q$ could be

considered, since some of their isomorphic curves can be translated one to the other.

The isogenous curve of a curve $E_{a,b}/\mathbb{F}_p$ with kernel $\{\mathcal{O},(0,0),(0,-b)\}$, according to Vélu formulae, has equation

$$E'/\mathbb{F}_p : y^2+axy+by = x^3-5abx-b(a^3+7b),$$

with 3-division polynomial $\Psi_3'(x) = (x+a^2/3)(x^3-9abx-b(a^3+27b))$. Then, considering the roots of this polynomial, the curve $E'/\mathbb{F}_q$ can be expressed in the model $E_{a,b}/\mathbb{F}_q$. Table 1 collects the isogenous curves obtained. In fact, for the case $v_3(q-1)=0$, notice that only the isogeny corresponding to the rational point is given.

Curve	Roots of $\psi_3'(x)$	Isogenous curve: case $v_3(q-1)=0$
$(1,\lambda)$	$-1/3,\beta$	$\left(1,\dfrac{(\beta+9\lambda)^4}{(6\beta^2+\beta-9\lambda)^3}\right)$ if $6\beta^2+\beta-9\lambda\neq 0$
		$(0,1)$ if $6\beta^2+\beta-9\lambda=0$
$(0,1)$	$-1/3,3$	$(1,1/24)$
Curve	Roots of $\psi_3(x)$	Isogenous curves: case $v_3(q-1)>0$
$(1,\lambda)$	0	$\left(1,\dfrac{1}{27}-\lambda\right)$
$(1,\lambda)$	$0,\beta_1,\beta_2,\beta_3$ $(\beta_i,\gamma_i)\in E_{1,\lambda}(\mathbb{F}_q)$	$\left(1,\dfrac{1}{27}-\lambda\right)$
		$\left(1,\dfrac{1}{27}-\dfrac{(\beta_i+2\gamma_i+\lambda)^4}{(6\beta_i^2+\beta_i+\lambda)^3}\right)$ if $6\beta_i^2+\beta_i+\lambda\neq 0$
		$(0,1)$ if $6\beta_i^2+\beta_i+\lambda=0$
$(0,1)$	$0,-1,\rho_1,\rho_2$	$(0,1),\ \left(1,-\dfrac{1}{216}\right),\ \left(1,-\dfrac{1}{216}\right),\ \left(1,-\dfrac{1}{216}\right)$
$(0,\delta_i)$	0	$(0,\delta_i)$

Table 1. Coefficients of the isogenous curves

3.2. Algorithm to obtain volcanoes of 3-isogenies.

Given an elliptic curve E over a finite field $\mathbb{F}_q$, the algorithm implemented in this work determines the height h of the volcano V_E in the non-regular case (recall that for the regular case, the height can be directly obtained from Theorem 1) and the length c of the crater. To do this, the core of the algorithm consists in finding an ascending path from the level where E is situated toward the crater of the volcano. Then, the length of the crater is obtained by going through all its vertices. More precisely, the algorithm proceeds as follows:

INPUT: An elliptic curve E over $\mathbb{F}_q$ in the form $y^2 + axy + by = x^3$.

OUTPUT: (k, h, c), where k is the level where E is placed on the volcano, h is the height of the volcano and c is the length of the crater.

---

1. *Determining the level of E in the volcano.*

$(n, r) :=$ 3-Sylow(E)
$\nu := v_\ell(q-1)$
if $r < n$ **or** $(r = n$ **and** $r \neq \nu)$ **then** $k := r$
else
  $s :=$Steps_To_Stability_Level(E)
  $k := r + s$
end if

2. *Reaching the crater of the volcano.*

$h := k$
while not Is_Crater_Curve(E) **do**
  $E :=$Ascending_Isogenous_Curve(E)
  $h := h + 1$
end while

3. *Going through the crater of the volcano.*

c:=1
$E_{curr} :=$Choose_Horizontal_Isogenous_Curve(E)
$E_{prev} := E$

while $E_{curr} \neq E$ **do**

c:=c+1

$E_{aux} := E_{curr}$

E_{curr} :=Horizontal_Isogenous_Curve(E_{curr}, E_{prev})

$E_{prev} := E_{aux}$

end while

return(k, h, c)

The functions that are called by the algorithm are the following:

- 3-Sylow: Returns the pair of integers (n, r), $r \leq n$, such that the 3-Sylow subgroup of E is isomorphic to $\mathbb{Z}/3^n\mathbb{Z} \times \mathbb{Z}/3^r\mathbb{Z}$. This function follows the polynomial time algorithm described in [**13**].
- Steps_To_Stability_Level: Takes as inputs the elliptic curve E and computes three paths of isogenies from E until reaching the stability level. Notice that, at least one of them will be a descending path. So the function returns the number of steps of this path, which gives the distance from E to the stability level.
- Is_Crater_Curve: Returns True if E is on the crater and False otherwise. In order to know if the curve belongs to the crater, its level on the volcano is computed. In the case of regular volcanoes, the level of the curve is given by the 3-Sylow parameters, taking into account that the height of the volcano is provided in Proposition 1. Otherwise, the level of the curves can be obtained by using the previous function. In this case, the crater is detected when the level of all the isogenous curves of E is equal or less than the level of E.
- Ascending_Isogenous_Curve: Computes the isogenous curves of E using the Vélu formulae and chooses the ascending one, by obtaining their level on the volcano.
- Choose_Horizontal_Isogenous_Curve: Computes the isogenous curves of E and returns one of the horizontal isogenies, by computing their level on the volcano.
- Horizontal_Isogenous_Curve: Given two curves E and E' such that there exists an horizontal isogeny $\mathcal{I}' \colon E' \to E$, this function returns the curve E'' for which there exists an horizontal isogeny $\mathcal{I} \colon E \to E''$ not dual to the isogeny $\mathcal{I}'$.

Notice that the level of a curve can be obtained by computing the descending paths towards the bottom level similarly to the procedure used by [**4**]. Nevertheless, our approach suggests an improvement of this method by using the algorithm proposed in [**13**]. Hence, computing descending paths can be completely avoided for the case of regular volcanoes, while for the non-regular ones only paths towards the stability level are required.

3.3. Some examples.

This algorithm has been implemented in LiDIA [**10**] and it has been used to test some volcanoes associated to different random elliptic curves over finite fields $\mathbb{F}_p$. Table 2 collects some examples of several volcanoes corresponding to curves $E_{1,\lambda}/\mathbb{F}_p$. The results obtained show, on the one hand, that their average heights are very small and, on the other hand, that the length of their craters can be huge. More precisely, empirical results point out that c can even achieve the value $\sqrt{p}$.

p	$v_3(p-1)$	λ	$v_3(\lvert E_{1,\lambda}\rvert)$	(h,c)
10007	0	130	3	$(0,132)$
131221	8	118403	8	$(4,4)$
4738294793	0	483209742	1	$(0,5255)$
5764865399	0	845734783	2	$(0,28193)$
6473810533	1	978203893	3	$(1,2337)$
$10^{14}+99$	2	4	2	$(1,810556)$
$10^{20}+441$	3	1	5	$(2,2)$
$10^{40}+921$	1	345789102	2	$(1,1)$
$10^{80}+129$	1	500	2	$(1,2)$

TABLE 2. Structure of some volcanoes $V_{E_{1,\lambda}}$ over $\mathbb{F}_p$

Furthermore, the algorithm has also been used to study the distribution of the volcanoes over a given finite field $\mathbb{F}_p$. Tables 3 and 4 provide the structure of all the volcanoes obtained for the primes $p = 227$ and $p = 229$, respectively, where m denotes the order of the curves such

that $v_3(m) \geq 1$. More precisely, for each possible structure determined by the pair (h, c), these tables list the corresponding volcanoes giving the parameters of one of the curves on its crater. Finally, last column of Table 4 shows the regularity of the volcano (notice that non-regular volcanoes are quite rare in the case $v_3(p-1) \geq 1$ and they even do not exist in the case $v_3(p-1) = 0$).

h	c	Curve parameters	m	$v_3(m)$
0	1	$(1, 199)$	198	2
0	1	$(1, 213)$	258	1
0	3	$(1, 10)$	204	1
0	3	$(1, 146)$	252	2
0	4	$(1, 33)$	228	1
0	5	$(1, 103)$	201	1
0	5	$(1, 25)$	213	1
0	5	$(1, 7),\ (1, 14)$	222	1
0	5	$(1, 1),\ (1, 5),\ (1, 8)$	228	1
0	5	$(1, 52),\ (1, 72)$	234	2
0	5	$(1, 6)$	243	5
0	5	$(1, 16)$	255	1
0	7	$(1, 26)$	207	2
0	7	$(1, 31)$	219	1
0	7	$(1, 53)$	237	1
0	7	$(1, 32)$	249	1
0	8	$(1, 13),\ (1, 57)$	210	1
0	8	$(1, 21),\ (1, 27)$	246	1

Table 3. Structure of the volcanoes over $\mathbb{F}_p$, $p = 227$, $v_3(p-1) = 0$

0	9	$(1, 11)$	204	1
0	9	$(1, 40)$	252	2
0	13	$(1, 24),\ (1, 58)$	216	3
0	13	$(1, 2),\ (1, 18)$	240	1
0	14	$(1, 4)$	225	2
0	14	$(1, 50)$	231	1

TABLE 3. Structure of the volcanoes over $\mathbb{F}_p$, $p = 227$, $v_3(p-1) = 0$ (continued)

h	c	Curve parameters	m	$v_3(m)$	Reg.
0	1	$(0, 134)$	201	1	yes
		$(0, 94)$	237	1	yes
0	2	$(1, 111)$	201	1	yes
		$(1, 20),\ (1, 92),\ (1, 96),\ (1, 116)$	204	1	yes
		$(1, 50),\ (1, 55),\ (1, 63),\ (1, 72),\ (1, 79),\ (1, 83)$	210	1	yes
		$(1, 24),\ (1, 40)$	213	1	yes
		$(1, 90),\ (1, 99)$	219	1	yes
		$(1, 56),\ (1, 80),\ (1, 87),\ (1, 112)$	222	1	yes
		$(1, 7),\ (1, 46),\ (1, 67),\ (1, 82),\ (1, 94),\ (1, 98)$	228	1	yes
		$(1, 5),\ (1, 75),\ (1, 89),\ (1, 119)$	231	1	yes
		$(1, 23),\ (1, 95),\ (1, 113)$	237	1	yes
		$(1, 3),\ (1, 35),\ (1, 41),\ (1, 48),\ (1, 58),\ (1, 62)$	240	1	yes

TABLE 4. Structure of the volcanoes over $\mathbb{F}_p$, $p = 229$, $v_3(p-1) = 1$

		$(1,65),\ (1,73),\ (1,91),\ (1,117)$	240	1	yes
		$(1,29),\ (1,31),\ (1,66),\ (1,76)$	246	1	yes
		$(1,37),\ (1,97)$	249	1	yes
		$(1,36),\ (1,100)$	255	1	yes
		$(1,45),\ (1,102)$	258	1	yes
1	1	$(1,38)$	207	2	yes
		$(1,6),\ (1,18),\ (1,49)$	234	2	yes
		$(1,33),\ (1,105) \cong (0,1)$	252	2	yes
1	2	$(1,4)$	252	2	yes
1	3	$(1,1)$	243	5	yes
1	4	$(1,2),\ (1,44)$	216	3	yes
2	1	$(1,60)$	225	2	no

Table 4. Structure of the volcanoes over $\mathbb{F}_p$, $p = 229$, $v_3(p-1) = 1$ (continued)

References

[1] A. O. L. Atkin, The number of points on an elliptic curve, Available at `http://listserv.nodak.edu/archives/nmbrthry.html`, February 1992.

[2] I. F. Blake, G. Seroussi and N. P. Smart, *"Elliptic curves in cryptography"*, Reprint of the 1999 original, London Mathematical Society Lecture Note Series **265**, Cambridge University Press, Cambridge, 2000.

[3] N. D. Elkies, Elliptic and modular curves over finite fields and related computational issues, in: *"Computational perspectives on number theory"* (Chicago, IL, 1995), AMS/IP Stud. Adv. Math. **7**, Amer. Math. Soc., Providence, RI, 1998, pp. 21–76.

[4] M. Fouquet and F. Morain, Isogeny volcanoes and the SEA algorithm, in: *"Algorithmic number theory"* (Sydney, 2002), Lecture Notes in Comput. Sci. **2369**, Springer, Berlin, 2002, pp. 276–291.

[5] S. D. GALBRAITH, Constructing isogenies between elliptic curves over finite fields, *LMS J. Comput. Math.* **2** (1999), 118–138 (electronic).
[6] D. HUSEMÖLLER, *"Elliptic curves"*, With an appendix by Ruth Lawrence, Graduate Texts in Mathematics **111**, Springer-Verlag, New York, 1987.
[7] D. R. KOHEL, Endomorphism rings of elliptic curves over finite fields, PhD thesis, University of California, Berkeley (1996).
[8] H. W. LENSTRA, JR., Complex multiplication structure of elliptic curves, *J. Number Theory* **56(2)** (1996), 227–241.
[9] R. LERCIER, Algorithmique des courbes elliptiques dans les corps finis, PhD Thesis, École Polytechnique, LIX (1997).
[10] LIDIA-GROUP, *"LiDIA Manual: A library for computational number theory"*, Edition 2.1.1, Tech. Univ. Darmstad, 2004, Available at `http://www.informatik.tu-darmstadt.de/TI/LiDIA`.
[11] J. MIRET, R. MORENO, A. RIO AND M. VALLS, Determining the 2-Sylow subgroup of an elliptic curve over a finite field, *Math. Comp.* **74(249)** (2005), 411–427 (electronic).
[12] J. MIRET, R. MORENO, D. SADORNIL, J. TENA AND M. VALLS, An algorithm to compute volcanoes of 2-isogenies of elliptic curves over finite fields, *Appl. Math. Comput.* **176(2)** (2006), 739–750.
[13] R. MORENO, Subgrupos de Sylow de las curvas elípticas definidas sobre cuerpos finitos, PhD Thesis, Universitat Politècnica de Catalunya (2005).
[14] R. SCHOOF, Elliptic curves over finite fields and the computation of square roots mod p, *Math. Comp.* **44(170)** (1985), 483–494.
[15] J. H. SILVERMAN, *"The arithmetic of elliptic curves"*, Graduate Texts in Mathematics **106**, Springer-Verlag, New York, 1986.
[16] J. VÉLU, Isogénies entre courbes elliptiques, *C. R. Acad. Sci. Paris Sér. A-B* **273** (1971), A238–A241.
[17] C. WITTMANN, Group structure of elliptic curves over finite fields, *J. Number Theory* **88(2)** (2001), 335–344.

Josep M. Miret, Rosana Tomàs and Magda Valls:
Departament de Matemàtica
Universitat de Lleida
25001 Lleida
Spain
E-mail address: `miret@eps.udl.es`
E-mail address: `rosana@eps.udl.es`
E-mail address: `magda@eps.udl.es`

Daniel Sadornil:
Departamento de Matemáticas
Universidad de Salamanca
37008 Salamanca
Spain
E-mail address: sadornil@usal.es

Juan Tena:
Departamento de Álgebra, Geometría y Topología
Universidad de Valladolid
47005 Valladolid
Spain
E-mail address: tena@agt.uva.es